

REMARKS/ARGUMENTS

Claims 3, 5-21, and 23 remain pending. Claims 24-28 are added.

In accordance with the instant claims:

- 1) Bandwidth thresholds can be set in terms of amount of data used, for example, over days, weeks, or even months, and are per user or group of users.
- 2) When bandwidth thresholds are exceeded, the real time bandwidth allocated to the specific user is either reduced or increased. It is not set to zero (or blocked) per Cromer.

The cited documents focus on dividing bandwidth in real time and blocking individual users' traffic or flow when they exceed real time bandwidth rates. Each example targets short-term (usually seconds or minutes) *network congestion* as established by short-term thresholds or real time available bandwidth.

The claimed invention attempts to target long term abusive users by reducing their consumption of network resources over extended periods of time – days, weeks, or months. It does not attempt to reduce congestion. When abusive users exceed their thresholds, the network allows them to continue to use the network while simultaneously making room for additional users.

The claimed invention also allows particular customers to have additional bandwidth for special circumstances. For example, if a user has important traffic, exceeding the threshold can be a trigger for increasing the available bandwidth or network resources to facilitate transmission of that critical traffic. When the increased bandwidth is no longer needed and no longer being used, the bandwidth may be decreased back to its normal level.

None of the cited documents teach or suggest these features. In response to a user violating bandwidth usage Cromer denies a clear-to-send signal to prevent transmission by placing the user on a restricted list. That is, transmission is blocked. It is not reduced. This is because Cromer is directed to *preventing traffic congestion*. As recognized in the Advisory Action, the decision whether to restrict access of a user can be based several factors such as the number of people using the system and how much bandwidth other people are using. Thus, for example, if the abusive user is the only user, then he will not be blocked.

As previously discussed, but reiterated for convenience, one feature of claim 3 is the imposition of a bandwidth *restriction* when certain conditions are met. Likewise, such restriction may be removed when such conditions are no longer present. The invention claimed

in claim 3 allows flexibility to the services provided to each subscriber on an individual basis depending on, for example, how much bandwidth the subscriber is allowed and whether such bandwidth may be increased or decreased. The bandwidth restriction does *not deny access or deny transmission* but merely slows down the user.

That is, a bandwidth restriction is a restriction of *the amount of data transmission* a subscriber is allowed per unit time. A bandwidth restriction would thus decrease the amount of data transmitted per unit time whereas removing the restriction would allow an increase of data transmitted per unit time. Bandwidth restrictions may be more or less severe depending on parameters of the subscriber or as recited in claim 3 “wherein each subscriber has its own defined level.” In contrast, Kiel simply grants or denies network access to the user. That is, Kiel is directed to a *prepaid* subscriber system with accounting done on each subscriber’s system. The system blocks access to the network when the subscriber’s *prepaid* account is depleted. Kiel’s system is similar to a prepaid calling card - when the money is depleted, the system turns off.

Attention is drawn to an example of how the method of the instant claim could work. If a user is allowed to send at 512 Kbps, but then exceeds 5GB of data transmitted in a week, his/her transmission rate (bandwidth) might be limited to 50 Kbps for the next week, if he/she then exceeded 7GB of data transmitted, the transmission rate might be limited to 10Kbps. In time and once the user is back in compliance, the rate would be restored to the original 512Kbps. (Note that this method allows the user to *keep using the network*, but just at a limited bandwidth.) Again, Kiel is directed allowing or not allowing access.

In response to a user violating bandwidth usage Cromer denies a clear-to-send signal to prevent transmission. Cromer does not restrict bandwidth - the amount of data transmitted per unit time. That is, Cromer describes control transmissions that are based on the ability to send a signal, which is *granted or denied*, and does not teach or suggest imposing a more restrictive bandwidth as recited in claim 3.

Thus Cromer prevents transmission as opposed to limiting bandwidth: “If the individual bandwidth utilization is greater than the threshold, then client is prevented from using the individual bandwidth until it is determined that the client is no longer greater than the threshold...” (emphasis added). Attention is also drawn to Cromer, page 3, lines 5-23, in

particular lines 17-19, which indicates that exceeding the threshold results in “prohibiting a clear-to-send response to a request-to-send by the particular client, ...” (Emphasis added).

In addition, Cromer merely describes supporting control of rates in *one direction*. In contrast, claim 23 recites, among other features, “when either the upstream or downstream balance of the account of a subscriber of the wireless network drops below a defined level, imposing a more restrictive bandwidth on that subscriber.” (Emphasis added). Even if properly combinable, Cromer fails to remedy the deficiencies of Kiel.

CONCLUSION

In view of the above remarks, this application is in condition for allowance.

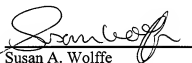
The Commissioner is authorized to charge our Deposit Account No. 19-0733 for any fees associated with this paper or application.

Respectfully submitted,

BANNER & WITCOFF, LTD.

Dated: November 3, 2008

By:



Susan A. Wolfe
Registration No. 33,568

1100 13th Street, N.W.
Washington, D.C. 20005
Tel: (202) 824-3000
Fax: (202) 824-3001